Fermat Numbers investigated for Primality and Factors

Allan Joseph R. Menezes,[1*]

112 Griselda Crescent, Brampton, L6S-1M3, Canada
*E-mail: amenezes007@gmail.com

Abstract

This paper proposes to explain the Lucas-Lehmer algorithm, which tests numbers for primality for Fermat Numbers.

Keywords:*Mersenne numbers, Lucas-Lehmer sequences, Fermat Numbers, prime, factor, GMP.*

AMS Subject Classication Code: 11A99

Introduction: Mersenne Numbers are numbers of the form $M_n = 2^n - 1$. These numbers have a polynomial time primality test called the Lucas-Lehmer Primality Test. Fermat Numbers are of the form $F_m = 2^n + 1$ where $n = 2^m - 1$. These numbers have a polynomial primality test called the Pepin's Test. We have devised an equivalent modified Lucas-Lehmer polynomial Primality Test for Fermat Numbers similar to Mersenne Numbers. The algorithms are similar. The software for testing the primality of Mersenne Numbers can be modified for both Mersenne and Fermat Numbers so that for both these types of numbers a single test could check for primality in polynomial time. The complexity of the Lucas-Lehmer Test for this is $O(n^2)$. For the Mersenne Numbers the underlying quadratic is $f(x) = x^2 - 4x + 1$ whereas for the Fermat Numbers it is $f(x) = x^2 - 5x + 1$

or $f(x) = x^2 - ax + 1$ where $a = 4, 5$ respectively. We have added additional GCD tests for factorization of these Fermat Numbers which can be deleted in the true primality test to make it more faster.

Definition 0.1. *The Lucas-Lehmer sequences $\{U_m\}_{m\geq 0}\{V_m\}_{m\geq 0}$ corresponding to $f(x) = x^2 - 5x + 1$ are defined by [1]*

$$U_m \equiv \frac{x^m - (a-x)^m}{x - (a-x)} (\mathrm{mod} f(x))$$
$$V_m \equiv x^m + (a-x)^m (\mathrm{mod} f(x))$$

THe alternative definition of the these Lucas-Lehmer sequences is:

Definition 0.2.

$$U_m \equiv \frac{\omega^m - \varpi^m}{\omega - \varpi} (\mathrm{mod} f(x))$$
$$V_m \equiv \omega^m + \varpi^m (\mathrm{mod} f(x))$$

where ω, ϖ are the roots of the quadratic $f(x) = x^2 - 5x + 1$.

Theorem 0.1 (The Lucas-Lehmer Variant for Fermat Numbers)**.** *Let V_m be the Lucas-Lehmer sequence as given in Definition (0.1). Let $v_0 = 5$ and $V_{2^{k+1}} = v_{k+1} = v_k^2 - 2$. Define $F_m = 2^{2^m} + 1$. Then F_m is prime iff*

$$v_{2^m - 2} \equiv 0(\mathrm{mod}(F_m))$$

Proof. ⇐ This proof is similar to [1], [10] Suppose F_m is composite and p is the smallest odd prime divisor of itself such that $p^2 < F_m$ and $(\frac{\Delta}{p}) = -1$. By the theorem's reverse hypothesis we have

$$V_{2^{2^m - 2}} \equiv 0(\mathrm{mod} F_m)$$

Since by the equivalent definition of $V_{2^{2^m-2}}$ where ω, ϖ are the roots of $f(x) = x^2 - 5x + 1$. Hence

$$\omega^{2^{2^m-2}} \equiv -\varpi^{2^{2^m-2}} (\bmod F_m)$$

$$\omega^{2^{2^m-1}} \equiv -1 (\bmod F_m)$$

$$\omega^{2^{2^m}} \equiv 1 (\bmod F_m)$$

Since by the theorem's reverse hypothesis the above exponent of ω is the least positive integer for which its modulus is one, therefore we conclude that the period of ω is 2^{2^m} which less than the order of multiplicative group of $F_{p^2} = p^2 - 1$. Hence $2^{2^m} < p^2 - 1$ or $F_m < p^2$ which is a contradiction of our assumption that if n is composite then for it's smallest divisor p, $p^2 < F_m$. Hence we conclude that F_m is prime. Thus, since $v_k = V_{2^k}$, all we have to show is that $v_{2^m-2} \equiv 0(\bmod(F_m))$ to show that F_m is prime. For the converse let $a = 5$, $F = 2^{(2^m-1)}$ and $N = F_m$ then $V_{2^{2^m}} \equiv 2(\bmod F_m)$.

$V_{\frac{F}{2}} \equiv V_{2^{(2^m-2)}} \equiv 0(\bmod F_m)$ and if $\gcd(3, F_m) = 1$ then letting $t = 2^m - 2$: By Euler's criterion since F_m is assumed prime:

$3^{\frac{F_m-1}{2}} \equiv (\frac{3}{F_m}) \equiv -1(\bmod F_m)$

$(x-1)^2 \equiv 3x(\bmod(f(x)))$

$(x-1)^{F_m-1} \equiv 1 \equiv (3x)^{\frac{F_m-1}{2}} \equiv -x^{2^{t+1}} (\bmod (f(x), F_m))$ or $x^{2^{t+1}} \equiv -1(\bmod (f(x), F_m))$

Similarly $(5-x)^{2^{t+1}} \equiv -1(\bmod(f(x), F_m))$. $V_{2^{t+1}} \equiv V_{2^t}^2 - 2 \equiv -2(\bmod(f(x), F_m))$. Setting $\frac{F}{2} \mid F_m - 1 = 2^{2^m}$ and we derive:

Hence $V_{2^{(2^m-2)}} \equiv 0(\bmod(f(x), F_m))$ iff F_m is prime. □

We follow the presentation [9], [1] and [3] in all of above.

$Fermat\_LL\_Test(F_m)$ is the a Variant of the Lucas-Lehmer algorithm for Fermat type numbers

```
Vars: $F_m, S_0, d1, d2$
Initialization:
Check $F_n$ for perfect powers and if it a product of twin primes and divisibilty by three and if so return $F_n$ composite with the factors.
$S_0 = a = 5$
$F_m = 2^n + 1$ where $n = 2^m$
    begin:
    For $i$ from 1 to $(n-2)$
        Determine $h_i = S_i \equiv S_{i-1}^2 - 2(\mathrm{mod}(F_m)$.
        $f_i = h_i^2 - a^2$   [3]
If $(d1 = \gcd(f_i, F_m) > 1) || (d2 = \gcd(f_i, F_m) > 1)$ —(A) then
            return $F_m$ is composite with factors $f_i$, $d1$,$d2$ if $d1 < F_m$ or $d2 < F_m$ —(A).
EndIf EndFor
//Test for primality or compositeness after the for loop:
If $(S_{(n-2)} == 0(\mathrm{mod} F_m))$
    return $F_m$ is prime
Else composite.
EndFermat_LL_Test()
```

For this Fermats Lucas-Lehmer Test start with 5 and square it and subtract 2 and do this to the resulting number again and so on to form the sequence $S_0, S_1, S_2, S_3 \cdots S_{n-2}$ where $S_0 = 5$,$S_1 = 5^2 - 2 = 23 \cdots$.

Note line marked (A) can be deleted from the above Lucas-Lehmer Primality Test for Fermat Numbers to make the test faster. Adding these lines and modifing their extent can make for primality and factorization of these Fermat Numbers. One can run the pure primality test without lines (A) on a Fermat Number F_m and factor only if it is determined composite saving time when these Fermat Numbers are prime. Similar Lucas-Lehmer Tests for Mersenne Numbers can be found in Number Theory Literature.

References and Notes

[1] Crandall,R., Pomerance C.
Prime Numbers: A Computational Perspective.
Springer-Verlag, Second Edition (2000) 37,143–144,145,182–184.

[2] Weisstein, Eric W. "Jacobi Symbol." From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/JacobiSymbol.html

[3] Ribenboim, Paulo
The Book of Prime Number Records.
Springer-Verlag, Second Edition, (1989) 41-46, 75-78.

[4] Graham Everest and Thomas Ward.
An Introduction to Number Theory
Springer-Verlag,(2000) 266-267

[5] Eric Bach and Jeffery Shallit
Algorithmic Number Theory, Volume 1, Efficient Algorithms

The MIT Press (1996) 113-114,215-216, 273-274

[6] GMP:GNU Multiple Precision Arithmetic Library
Torbjörn Granlund and the GMP development team
http : //gmplib.org

[7] GCC:GNU C Compiler
http : //gcc.gnu.org

[8] B.W. Brewer
Tests for Primality.
pp757-763

[9] Seminar with Dr. V.K. Murty
Ganita Laboratory
University of Toronto,
Mississauga,
Ontario
Canada
June, 2008

[10] D.H. Lehmer. *An Extended theory of Lucas' Functions.* Annals of Mathematics. Second Series. Vol. 131. No. 3(Jul. 1930) pp419-448,p442.

[11] Tony Reix. *A LLT-like test for proving the primality of Fermat numbers*. pp1,6.

[12] D. Knuth. *TeX. A document formatting language*

[13] M. Agrawal, N. Kayal, N. Saxena. *PRIMES is in P*. Dept. of Computer Science and Engineering, Indian Institute of Technology, Kanpur.

[14] http://mathworld.wolfram.com/PrimeCountingFunction.html

[15] http://www.sagemath.org